AO 106A (08/18) Application for a Warrant by Telephone or Other Reliable Electronic Means

UNITED STATES DISTRICT COURT

for the

Northern District of New York

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

INFORMATION ASSOCIATED WITH A GOOGLE ACCOUNT THAT IS STORED AT PREMISES CONTROLLED BY GOOGLE LLC

Case No. 1:22-MJ-180-DJS

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A.

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 875(c) (	Interstate Communications with a Threat to Injure

The application is based on these facts:

See attached affidavit.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Jason D. Manchuck, TFO FBI
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone *(specify reliable electronic means).*

Date: 4/14/2022

Judge's signature

City and state: Albany, NY

Hon. Daniel J. Stewart, U.S. Magistrate Judge
Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF NEW YORK

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH THE GOOGLE ACCOUNT KYOSHOSCORPIONXXL@GMAIL.COM THAT IS STORED AT PREMISES CONTROLLED BY GOOGLE LLC	Case No. 1:22-MJ-180-DJS Filed Under Seal

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR SEARCH WARRANT

I, **Jason D. Manchuck**, being duly sworn, hereby depose and state as follows:

INTRODUCTION

1. I make this affidavit in support of an application for a warrant to search information associated with a certain account—**kyoshoscorpionxxl@gmail.com** (the "Target Account")—that is stored at premises owned, maintained, controlled, or operated by Google LLC ("Google" or "Provider"), an electronic communications service and/or remote computing service provider headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(l)(A), and 2703(c)(l)(A) to require Google to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am an Investigator with the New York State Police, Bureau of Criminal Investigation, currently assigned to the New York State Intelligence Center (NYSIC), with the Division of the New York State Police. Additionally, I am a Task Force Officer with the Federal

Bureau of Investigation, Albany, New York Field Office and am assigned to the Joint Terrorism Task Force.

3. I have been employed as a Police Officer with the New York State Police since December 1, 2008 and was subsequently promoted to the rank of Investigator with the Bureau of Criminal Investigation on September 11, 2014. While working as a Trooper, and later as an Investigator, I have worked on several hundred criminal and non-criminal investigations. Many of these range from direct contribution through case agent and/or criminal investigation autonomy, to multiagency operations, involving the use of special details, as appropriate and necessary. These investigations include being the case agent responsible for threats, assaults, sexual assaults, child abuse/endangerment, larcenies, frauds and burglaries, robberies, drug investigations (focusing on the development of and use of confidential informants and working in an undercover capacity), missing persons, and homicides. Although typical for investigations to include traditional complainant-generated incidents, others involve proactive or self-initiated investigations through interviews/interrogations, the development of confidential informants, and the employment of covert physical and electronic surveillance techniques in furtherance of continued investigative action. Additionally, I have routinely been the affiant on and subsequently executed numerous search warrants relative to these investigations. I am a law enforcement officer of the United States within the meaning of Title 18, United States Code, Section 2510(7), and am authorized to apply for and execute search warrants and arrest warrants for offenses enumerated in Title 18 of the United States Code.

4. As a Trooper, after initial training, I was afforded the opportunity to attend numerous training initiatives to include the Advanced Criminal Interdiction Training and the New York State Police Undercover Operations School. As an Investigator, I have attended additional

trainings including but not limited to the New York State Police Electronic Surveillance & Title III Eavesdropping Warrant Training, the New York State Police Advanced Search Warrant Training, the New York State Police Basic Criminal Investigation School, the New York State Police Basic Crisis Negotiator School, and the National Children's Advocacy Center Training–Forensic Interviewing of Children Training.

5. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. I have not included every fact about this investigation. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all my knowledge about this matter. Where statements of others are related in this affidavit, they are related in substance and in part.

6. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 875(c) (Interstate Communications with a Threat to Injure) have been committed by unknown persons. There is probable cause to search the Target Account, further described in Attachment A, for evidence and instrumentalities of these crimes, as further described in Attachment B.

JURISDICTION

7. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. § 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

8. As set forth below, this affidavit relates to a criminal investigation regarding violations of 18 U.S.C. § 875 (Interstate Communications with a Threat to Injure), by an individual

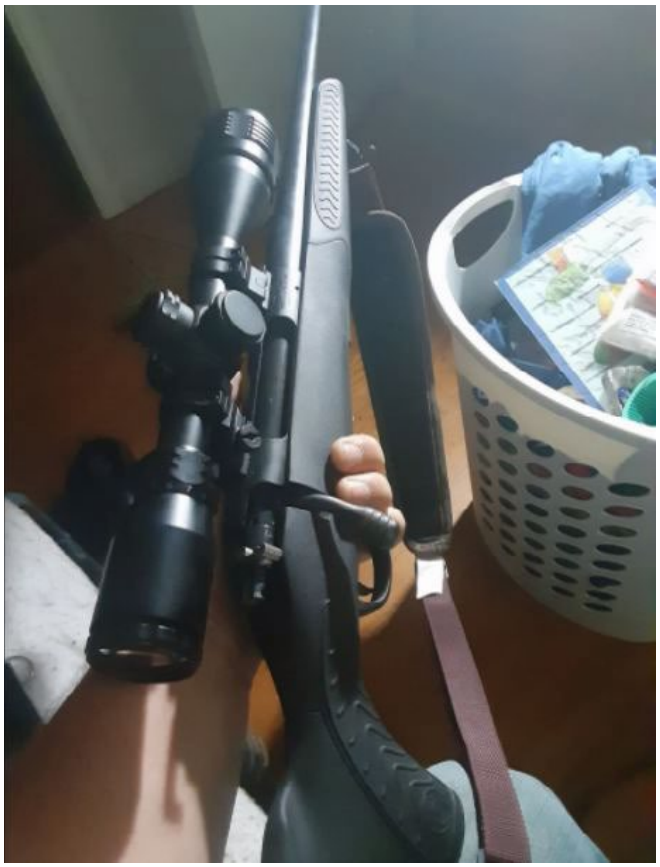
who sent a threatening communication on December 6, 2021, to A.D., a U.S. Army Recruiter in Cedar Hills, Texas.

Email Threat on December 8, 2021

9. In December 2021, A.D. was a Staff Sergeant and U.S. Army Recruiter assigned to the Cedar Hills Recruiting Station in Cedar Hills, Texas. The Cedar Hills Recruiting Office was responsible for thirteen zip codes in the immediate area of Cedar Hill, Texas, including Cedar Hill, TX (zip codes 75104, 75137), Duncanville, TX (zip codes 75236, 75249, 75116, 75138, and 75137), Desoto, TX (zip codes 75115 and 75123), Lancaster, TX (zip codes 75134 and 75146), and Wilmer, TX (zip codes 75141, 75172).

10. On December 6, 2021, A.D sent a mass recruiting email to a large distribution list for the Cedar Hill area as part of social media recruiting operations. The distribution list contained numerous email addresses from a database within the U.S. Army's system.

11. That same day, on December 6, 2021 at 10:46:40 PM, A.D. received an email from the Target Account (with a listed name as "Firefly Summer") with subject line "NIGGER LOVER" and stated, "NIGGER LOVER WATCH YOUR BACK!." Attached to the email from the Target Account was an image file titled "Screenshot 2021-10-21 5.51.19 PM.png" depicting an unknown individual holding a rifle, as seen below:



12. When interviewed by law enforcement on January 20, 2022, A.D. reported that he was accustomed to receiving threatening emails containing derogatory and racist comments but the email he received from the Target Account on December 7, 2021 was the first time a message had a picture attached to it, which alarmed A.D. After receiving the email, A.D. reported it to his chain of command, who then reported it to law enforcement. When asked, A.D. did not recall any abnormal behavior from anyone who visited the recruiting station over the previous few months. A.D. and his supervisor attempted to research the email address that sent the message using their own databases but did not find any information to identify the person who sent the email. A.D. reported that he did not have access to any records regarding the identity of individuals associated with email addresses on the U.S. Army's recruiting distribution lists. It is currently unknown how the Target Account user identified A.D.'s email or why A.D. was targeted.

13. Based on records produced by Google in response to a grand jury subpoena, the Target Account was registered on March 29, 2016 to a subscriber named "Firefly Summer" from an IP address 24.105.218.231.[1] The Target Account lists a recovery e-mail of goldenlion413@outlook[.]com ("Golden Lion Outlook Account") with no listed phone number or recovery SMS number. As of January 25, 2022 when Google produced records, the Target Account had been active and had logged-in as recently as January 25, 2022 from IP address 24.148.113.195. According to Google records, the Target Account utilizes the following Google Services: Web & App Activity, Gmail, Google Hangouts, Chromeos Login, Google Chrome Sync, Google Play Music, YouTube, Google Drive, Android, Google Docs, Google Play, Google Calendar, Google Keep, Google My Maps, Location History, Google Photos, and Dynamite.

14. Because the Target Accountholder sent a threatening email message, and included a photo image with that message, and the subpoena return for the Target Account reveals that the Target Account user uses Gmail, Google Drive, and Google Photos, among other services, the evidence of the crime may have been backed up to Google servers. Likewise, the Location History and Google Map information may contain information indicating where the Target Accountholder was when the email was sent. Other Google services utilized by the Target Account may reveal user attribution information to identify the perpetrator.

15. On January 26, 2022, a request was sent to Google to preserve, pursuant to Title 18, United States Code, Section 2703(f), all records and other evidence in its possession related to the Target Account.

[1] That IP address is associated with the Internet Service Provider Mid-Hudson Cablevision Inc. at a location in New York.

Other Records Associated with the Target Account and the Golden Lion Outlook Account

16. Based on records produced by Microsoft Corporation in response to a grand jury subpoena, a Skype account associated with the Golden Lion Outlook Account has a display name "thomas powers."[2] According to Microsoft, the Golden Lion Outlook Account utilizes the following Microsoft services: Mail, Xbox Live, Skype, Windows Live One Drive, and Office 365 Delve. According to Microsoft records, the Golden Lion Outlook Account was last modified on December 11, 2021 when there was a login from IP address 24.148.113.195.

17. Based on records produced by Meta Platforms Inc. formerly known as Facebook Inc. in response to a grand jury subpoena, an Instagram account was registered in the name of "Huelyn Duvall" on December 25, 2020 from IP address 24.148.113.195 with a registered email address as the Target Account, and the vanity name "goldenlion413" (the "Golden Lion Instagram Account"). Based on records produced by Meta as of January 24, 2022, there was recent login activity on the Golden Lion Instagram Account on January 17, 2022 from IP address 24.148.113.195.

18. Based on records produced by Twitter Inc., a Twitter account was registered to username "FireflySummer3" for an account in the name of "Huelyn Duvall" on August 12, 2021, from IP address 24.148.113.195 with a registered email address as the Target Account (the "Firefly Twitter Account"). Based on a review of publicly available content for the Firefly Twitter Account, law enforcement was unable to identify any public posts, or any location associated with the user.

19. Based on records produced by Mid-Hudson Cablevision Inc. in response to a grand jury subpoena, IP address 24.148.113.195 (the IP address associated with recent activity on the

[2] Microsoft records also show that the Golden Lion Outlook Account is associated with a user with listed name "napolian picknee."

Target Account, the Golden Lion Outlook Account, the Golden Lion Instagram Account, and the Firefly Twitter Account) is associated with an account for M. Powers at a service address at 5207 Route 32, Apt. B6, Catskill, New York.[3] Based on public sources, Thomas Powers is believed to be related to M. Powers.

20. On February 18, 2022, an agent with the FBI conducted additional open-source searches for "goldenlion413," which revealed a July 2006 post on a forum "forwardlook.net" titled "[Chrysler300] brake booster check valve quest." The post was made from "goldenlion413@xxxxxxx." At the end of the post, user goldenlion413 stated, "thanks for any help *tom from catskill new york*." (emphasis added).

BACKGROUND ABOUT GOOGLE

21. Google is the provider of the Target Account, an internet-based account identified by **kyoshoscorpionxxl@gmail.com**, with Google Account ID 133097682618.

22. Google is a United States company that offers to the public through its Google Accounts a variety of online services, including email, cloud storage, digital payments, and productivity applications, which can be accessed through a web browser or mobile applications. Google also offers to anyone, whether or not they have a Google Account, a free web browser called Google Chrome, a free search engine called Google Search, a free video streaming site called YouTube, a free mapping service called Google Maps, and a free traffic tracking service called Waze. Many of these free services offer additional functionality if the user signs into their Google Account.

23. In addition, Google offers an operating system ("OS") for mobile devices, including cellular phones, known as Android. Google also sells devices, including laptops, mobile phones,

[3] Catskill, New York is in Greene County, within the Northern District of New York.

tablets, smart speakers, security cameras, and wireless routers. Users of Android and Google devices are prompted to connect their device to a Google Account when they first turn on the device, and a Google Account is required for certain functionalities on these devices.

24. Signing up for a Google Account automatically generates an email address at the domain gmail.com. That email address will be the log-in username for access to the Google Account.

25. Google advertises its services as "One Account. All of Google working for you." Once logged into a Google Account, a user can connect to Google's full suite of services offered to the general public, described in further detail below. In addition, Google keeps certain records indicating ownership and usage of the Google Account across services, described further after the description of services below.

a. *Gmail*. Google provides email services (called Gmail) to Google Accounts through email addresses at gmail.com or enterprise email addresses hosted by Google. Gmail can be accessed through a web browser or a mobile application. Additional email addresses ("recovery," "secondary," "forwarding," or "alternate" email addresses) can be associated with the Google Account by the user. Google preserves emails associated with a Google Account indefinitely, unless the user deletes them.

b. *Contacts.* Google provides an address book for Google Accounts through Google Contacts. Google Contacts stores contacts the user affirmatively adds to the address book, as well as contacts the user has interacted with in Google products. Google Contacts can store up to 25,000 contacts. Users can send messages to more than one contact at a time by manually creating a group within Google Contacts or

communicate with an email distribution list called a Google Group. Users have the option to sync their Android mobile phone or device address book with their account so it is stored in Google Contacts. Google preserves contacts indefinitely, unless the user deletes them. Contacts can be accessed from the same browser window as other Google products like Gmail and Calendar.

c. *Calendar.* Google provides an appointment book for Google Accounts through Google Calendar, which can be accessed through a browser or mobile application. Users can create events or RSVP to events created by others in Google Calendar. Google Calendar can be set to generate reminder emails or alarms about events or tasks, repeat events at specified intervals, track RSVPs, and auto-schedule appointments to complete periodic goals (like running three times a week). A single Google Account can set up multiple calendars. An entire calendar can be shared with other Google Accounts by the user or made public so anyone can access it. Users have the option to sync their mobile phone or device calendar so it is stored in Google Calendar. Google preserves appointments indefinitely, unless the user deletes them. Calendar can be accessed from the same browser window as other Google products like Gmail and Calendar

d. *Messaging.* Google provides several messaging services including Duo, Messages, Hangouts, Meet, and Chat. These services enable real-time text, voice, and/or video communications through browsers and mobile applications, and also allow users to send and receive text messages, videos, photos, locations, links, and contacts. Google may retain a user's messages if the user hasn't disabled that feature or deleted the messages, though other factors may also impact retention. Google does

not retain Duo voice calls, though it may retain video or voicemail messages.

e. *Drive and Keep*. Google Drive is a cloud storage service automatically created for each Google Account. Users can store an unlimited number of documents created by Google productivity applications like Google Docs (Google's word processor), Google Sheets (Google's spreadsheet program), Google Forms (Google's web form service), and Google Slides, (Google's presentation program). Users can also upload files to Google Drive, including photos, videos, PDFs, and text documents, until they hit the storage limit. Users can set up their personal computer or mobile phone to automatically back up files to their Google Drive Account. Each user gets 15 gigabytes of space for free on servers controlled by Google and may purchase more through a subscription plan called Google One. In addition, Google Drive allows users to share their stored files and documents with up to 100 people and grant those with access the ability to edit or comment. Google maintains a record of who made changes when to documents edited in Google productivity applications. Documents shared with a user are saved in their Google Drive in a folder called "Shared with me." Google preserves files stored in Google Drive indefinitely, unless the user deletes them. Google Keep is a cloud-based notetaking service that lets users take notes and share them with other Google users to view, edit, or comment. Google Keep notes are stored indefinitely, unless the user deletes them.

f. *Photos.* Google offers a cloud-based photo and video storage service called Google Photos. Users can share or receive photos and videos with others. Google Photos can be trained to recognize individuals, places, and objects in photos and videos

and automatically tag them for easy retrieval via a search bar. Users have the option to sync their mobile phone or device photos to Google Photos. Google preserves files stored in Google Photos indefinitely, unless the user deletes them.

g. *Maps.* Google offers a map service called Google Maps which can be searched for addresses or points of interest. Google Maps can provide users with turn-byturn directions from one location to another using a range of transportation options (driving, biking, walking, etc.) and real-time traffic updates. Users can share their real-time location with others through Google Maps by using the Location Sharing feature. And users can find and plan an itinerary using Google Trips. A Google Account is not required to use Google Maps, but if users log into their Google Account while using Google Maps, they can save locations to their account, keep a history of their Google Maps searches, and create personalized maps using Google My Maps. Google stores Maps data indefinitely, unless the user deletes it.

h. *Location History.* Google collects and retains data about the location at which Google Account services are accessed from any mobile device, as well as the periodic location of Android devices while they are in use. This location data can derive from a range of sources, including GPS data, Wi-Fi access points, cell-site locations, geolocation of IP addresses, sensor data, user searches, and Bluetooth beacons within range of the device. According to Google, this location data may be associated with the Google Account signed-in or registered to the device when Location Services are activated on the device and the user has enabled certain global settings for their Google Account, such as Location History or Web & App Activity tracking. The data retained may be both precision location data, like

latitude and longitude coordinates derived from GPS, and inferential location data, such as the inference that a Google Account is in New York because it conducts a series of searches about places to eat in New York and directions from one New York location to another. Precision location data is typically stored by Google in an account's Location History and is assigned a latitude-longitude coordinate with a meter radius margin of error. Inferential data is stored with an account's Web & App Activity. Google maintains these records indefinitely for accounts created before June 2020, unless the user deletes it or opts to automatically delete their Location History and Web & App Activity after three or eighteen months. Accounts created after June 2020 auto-delete Location History after eighteen months unless the user affirmatively changes the retention setting to indefinite retention or auto-deletion at three months.

i. *Google Pay.* A subsidiary of Google, Google Payment Corporation, provides Google Accounts an online payment service called Google Pay (previously Google Wallet), which stores credit cards, bank accounts, and gift cards for users and allows them to send or receive payments for both online and brick-andmortar purchases, including any purchases of Google services. Users may delete some data associated with Google Pay transactions from their profile, but Google Payment Corporation retains some records for regulatory purposes.

j. *Chrome and My Activity.* Google offers a free web browser service called Google Chrome which facilitates access to the Internet. Chrome retains a record of a user's browsing history and allows users to save favorite sites as bookmarks for easy access. If a user is logged into their Google Account on Chrome and has the

appropriate settings enabled, their browsing history, bookmarks, and other browser settings may be saved to their Google Account in a record called My Activity. My Activity also collects and retains data about searches that users conduct within their own Google Account or using the Google Search service while logged into their Google Account, including voice queries made to the Google artificial intelligence-powered virtual assistant Google Assistant or commands made to Google Home products. Google also has the capacity to track the websites visited using its Google Chrome web browser service, applications used by Android users, ads clicked, and the use of Google applications by iPhone users. According to Google, this search, browsing, and application use history may be associated with a Google Account when the user is logged into their Google Account on the browser or device and certain global settings are enabled, such as Web & App Activity. Google Assistant and Google Home voice queries and commands may also be associated with the account if certain global settings are enabled, such as Voice & Audio Activity tracking. Google maintains these records indefinitely for accounts created before June 2020, unless the user deletes them or opts in to automatic deletion of their location history every three or eighteen months. Accounts created after June 2020 auto-delete Web & App Activity after eighteen months unless the user affirmatively changes the retention setting to indefinite retention or auto-deletion at three months.

k. *Google Play.* Google Accounts can buy electronic media, like books, movies, and music, and mobile applications from the Google Play Store. Google Play records can include records of whether a particular application has been or is currently installed on a device. Users cannot delete records of Google Play transactions

without deleting their entire Google Account.

l. *Google Voice.* Google offers a service called Google Voice through which a Google Account can be assigned a telephone number that can be used to make, record, and forward phone calls and send, receive, store, and forward SMS and MMS messages from a web browser, mobile phone, or landline. Google Voice also includes a voicemail service. Records are stored indefinitely, unless the user deletes them.

m. *YouTube.* Google also offers a video platform called YouTube that offers Google Accounts the ability to upload videos and share them with others. Users can create a YouTube channel where they can upload videos, leave comments, and create playlists available to the public. Users can subscribe to the YouTube channels of others, search for videos, save favorite videos, like videos, share videos with others, and save videos to watch later. More than one user can share control of a YouTube channel. YouTube may keep track of a user's searches, likes, comments, and change history to posted videos. YouTube also may keep limited records of the IP addresses used to access particular videos posted on the service. Users can also opt into a setting to track their YouTube Watch History. For accounts created before June 2020, YouTube Watch History is stored indefinitely, unless the user manually deletes it or sets it to auto-delete after three or eighteen months. For accounts created after June 2020, YouTube Watch History is stored for three years, unless the user manually deletes it or sets it to auto-delete after three or eighteen months.

26. Google integrates its various services to make it easier for Google Accounts to access the full Google suite of services. For example, users accessing their Google Account through their browser can toggle between Google Services via a toolbar displayed on the top of

most Google service pages, including Gmail and Drive. Google Hangout, Meet, and Chat conversations pop up within the same browser window as Gmail. Attachments in Gmail are displayed with a button that allows the user to save the attachment directly to Google Drive. If someone shares a document with a Google Account user in Google Docs, the contact information for that individual will be saved in the user's Google Contacts. Google Voice voicemail transcripts and missed call notifications can be sent to a user's Gmail account. And if a user logs into their Google Account on the Chrome browser, their subsequent Chrome browser and Google Search activity is associated with that Google Account, depending on user settings.

27. When individuals register with Google for a Google Account, Google asks users to provide certain personal identifying information, including the user's full name, telephone number, birthday, and gender. If a user is paying for services, the user must also provide a physical address and means and source of payment.

28. Google typically retains and can provide certain transactional information about the creation and use of each account on its system. Google captures the date on which the account was created, the length of service, log-in times and durations, the types of services utilized by the Google Account, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via Google's website or using a mobile application), details about the devices used to access the account, and other log files that reflect usage of the account. In addition, Google keeps records of the Internet Protocol ("IP") addresses used to register the account and accept Google's terms of service, as well as the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the Google Account.

29. Google maintains the communications, files, and associated records for each service used by a Google Account on servers under its control. Even after a user deletes a communication or file from their Google Account, it may continue to be available on Google's servers for a certain period of time.

30. In my training and experience, evidence of who was using a Google account and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion. Here, the individual who sent the threatening message under investigation was identified only as "Firefly Summer" and by the Target Account and did not provide his name or signature. As a result, the exact identity of the user of the Target Account, and the target of the investigation, is currently unknown. The data sought here would therefore help establish the identity of who was responsible for the December 6, 2021 email, and his motive for sending that message.

31. Based on my training and experience, messages, emails, voicemails, photos, videos, documents, and internet searches are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation. Thus, stored communications and files connected to a Google Account may provide direct evidence of the offenses under investigation. For example, in this case, the perpetrator sent an image as part of the interstate threat communicated to A.D. and any additional information about photos and emails sent or received by the user of the Target Account may provide information about the communication of the offenses under investigation and which may be stored on Google servers.

32. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Google can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation. Here, the investigation concerns an interstate threat by a person currently unknown. The "user attribution" evidence contained in the Target Account would allow investigators to confirm the identity of the investigation, establish attribution as to the perpetrator(s), and locate that target through the review of user content and GPS location information in the Target Account.

33. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (*e.g.,* information indicating a plan to commit a crime), or consciousness of guilt (*e.g.,* deleting account information in an effort to conceal evidence from law enforcement).

34. Other information connected to the use of a Google account may lead to the discovery of additional evidence. For example, the apps downloaded from the Google Play store may reveal services used in furtherance of the crimes under investigation or services used to

communicate with co-conspirators. For example, apps for certain retail stores (e.g. Amazon, eBay) might reveal information related to the purchase and sale of firearms or explosives used to carry out the particular threat; apps for certain payment processors and financial institutions (e.g. PayPal, Block) may reveal how those items were purchased; and apps used for social media and messaging may reveal other methods of communication used by the target to communicate with potential victims or conspirators about the email being investigated, or other related threatening communications. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

35. This investigation concerns an interstate threat sent by a user of the Target Account and the Target Account utilizes various Google services. Therefore, Google's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Google services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users. In fact, even if subscribers provide Google with false information about their identities, that false information often nevertheless provides clues to their identities, locations, or illicit activities.

EXECUTION AT ANY TIME DAY OR NIGHT

36. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Apple. Because the warrant will be served on Apple, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

CONCLUSION

37. Based on the forgoing, I request that the Court issue the proposed search warrant.

Attested to by the affiant:

Jason D. Manchuck
Task Force Officer
Federal Bureau of Investigation

I, the Honorable Daniel J. Stewart, United States Magistrate Judge, hereby acknowledge that this affidavit was attested by the affiant by telephone on April 14, 2022 in accordance with Rule 4.1 of the Federal Rules of Criminal Procedure.

Hon. Daniel J. Stewart
United States Magistrate Judge

ATTACHMENT A

Property To Be Searched

This warrant applies to information associated with the Google account **kyoshoscorpionxxl@gmail.com** (Google Account ID 133097682618) that is stored at premises owned, maintained, controlled, and/or operated by Google LLC, a company that accepts service of legal process and is headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043.

ATTACHMENT B

Particular Things To Be Seized

I. Information To Be Disclosed By Google LLC ("Google" or "Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to Google, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Google is required to disclose the following information to the government for the account or identifier listed in Attachment A (the "**Target Account**") for the time period **December 1, 2021 to present**, unless otherwise indicated:

a. All business records and subscriber information, in any form kept, pertaining to the Target Account, including:

1. Names (including subscriber names, usernames, and screen names);
2. Addresses (including mailing addresses, residential addresses, business addresses, and email addresses, including alternate and recovery email addresses);
3. Telephone numbers, including SMS recovery and alternate sign-in numbers;
4. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol ("IP") addresses) associated with those sessions, including log-in IP addresses;

5. Telephone or instrument numbers or other subscriber numbers or identities, including any temporarily assigned network address, SMS recovery numbers, Google Voice numbers, and alternate sign-in numbers

6. Length of service (including start date and creation IP) and types of service utilized;

7. Means and source of payment (including any credit card or bank account number); and

8. Change history.

b. All device information associated with the Account, including but not limited to, manufacture names, model numbers, serial number, media access control (MAC) addresses, international mobile equipment identifier (IMEI) numbers, FCC ID numbers, Android IDs, and telephone numbers;

c. Records of user activity for each connection made to or from the Account(s), including, for all Google services, the date, time, length, and method of connection, data transfer volume, usernames, source and destination IP address, name of accessed Google service, and all activity logs;

d. *Gmail.* The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, draft emails, and deleted emails; attachments; the source and destination addresses associated with each email; the size, length, and timestamp of each email; and true and accurate header information including the actual IP addresses of the sender and recipients of the emails; as well as all forwarding or fetching accounts relating to the accounts.

e. *Contacts.* Any records pertaining to the user's contacts, including: address books; contact lists; social network links; groups, including Google Groups to which the user belongs or communicates with; user settings; and all associated logs and change history.

f. *Calendar.* Any records pertaining to the user's calendar(s), including: Google Calendar events; Google Tasks; reminders; appointments; invites; and goals; the sender and recipients of any event invitation, reminder, appointment, or task; user settings; and all associated logs and change history

g. *Messaging.* The contents of all text, audio, and video messages associated with the account, including Chat, Duo, Hangouts, Meet, and Messages (including SMS, MMS, and RCS), in any format and however initially transmitted, including, but not limited to: stored, deleted, and draft messages, including attachments and links; the source and destination addresses associated with each communication, including IP addresses; the size, length, and timestamp of each communication; user settings; and all associated logs, including access logs and change history.

h. *Google Drive and Keep.* The contents of all records associated with the account in Google Drive (including Docs, Sheets, Forms, and Slides) and Google Keep, including: files, folders, media, notes and note titles, lists, applications for any Android-user, and other data uploaded, created, stored, or shared with the account including drafts and deleted records; third-party application data and backups for any Android-user; SMS data and device backups; the creation and change history of each record; accounts with access to or which previously accessed each record;

any location, device, other Google service (such as Google Classroom or Google Group), or third party application associated with each record; and all associated logs, including access logs and IP addresses, of each record.

i. *Photos.* The contents of all media associated with the account in Google Photos, including: photos, GIFs, videos, animations, collages, icons, or other data uploaded, created, stored, or shared with the account, including drafts and deleted records; accounts with access to or which previously accessed each record; any location, device, or third-party application data associated with each record; and all associated logs of each record, including the creation and change history, access logs, and IP addresses.

j. *Maps and Trips*. All maps data associated with the account, including Google Maps and Google Trips, including: all saved, starred, and privately labeled locations; search history; routes begun; routes completed; mode of transit used for directions; My Maps data; accounts and identifiers Google - ISP List DOJ – CCIPS Last updated 8/6/20 7 receiving or sending Location Sharing information to the account; changes and edits to public places; and all associated logs, including IP addresses, location data, and timestamps, and change history.

k. *Location History & Web & App Activity.* All Location History and Web & App Activity indicating the location at which the account was active, including the source of the data, date and time, latitude and longitude, estimated accuracy, device and platform, inferences drawn from sensor data (such as whether a user was at rest, walking, biking, or in a car), and associated logs and user settings, including Timeline access logs and change and deletion history

l. *Google Pay.* All payment and transaction data associated with the account, such as Google Pay and Google Wallet, including: records of purchases, money transfers, and all other transactions; address books; stored credit; gift and loyalty cards; associated payment cards, including any credit card or bank account number, PIN, associated bank, and other numbers; and all associated access and transaction logs, including IP address, time stamp, location data, and change history.

m. *Browsing, Search, and Application History.* All Internet search and browsing history, and application usage history, including Web & App Activity, Voice & Audio History, Google Assistant, and Google Home, including: search queries and clicks, including transcribed or recorded voice queries and Google Assistant responses; browsing history, including application usage; bookmarks; passwords; autofill information; alerts, subscriptions, and other automated searches, including associated notifications and creation dates; user settings; and all associated logs and change history.

n. *Google Play.* All activity relating to Google Play, including: downloaded, installed, purchased, used, and deleted applications, movies, music, television shows, books, magazines, and other files; details of the associated device and Android ID for each application, medium, or file; payment transactions; user settings; and all associated logs, including IP addresses, timestamps, and change history.

o. *Google Voice.* All Google Voice records associated with the account, including forwarding and other associated telephone numbers, connection records; call

detail records; SMS and MMS messages, including draft and deleted messages; voicemails, including deleted voicemails; user settings; and all associated logs, including access logs, IP addresses, location data, timestamps, and change history.

p. *YouTube.*

1. Subscriber Information: Records associated with the account's YouTube registration, including the account's display name, IP logs, channel ID, account registration information, and registration email.
2. Contents: The contents of all media associated with the account on YouTube, whether active, deleted, or in draft, including: copies of videos and other media only if uploaded to, saved to, shared by or shared with the account; playlists; connected applications; associated URLs for each record; creation and change history; privacy settings for each record; and all associated logs, including IP addresses, locations, timestamps, and device identifiers;
3. Watch History: A record of the account's YouTube Watch History, including: accessed URLs and their associated duration, privacy settings, edits, comments, likes, chats, and other interactions, including associated URLs; search history; channels; subscriptions; subscribers, friends, and other contacts; IP addresses, change history, location information, and uploading account or identifier; the logs for each access by the account, including IP address, location, timestamp, and device identifier; and change history.

q. *Support.* All records of communications between Google and any person regarding the Target Account, including contacts with support services and records of actions taken.

r. *Complaints.* Information about any complaint, alert, or other indication of malware, fraud, or terms of service violation related to a Target Account or associated user(s), including any memoranda, correspondence, investigation files, or records of meetings or discussions about the Target Account or associated user(s) (but not including confidential communications with legal counsel).

The Provider is hereby ordered to disclose the above information to the government within **14 days** of service of this warrant.

II. Information To Be Seized By The Government

All information described above in Section I that constitutes evidence and/or instrumentalities of violations of 18 U.S.C. §§ 875 (Interstate Communications with Threat to Injure), by an individual who sent a threatening communication on December 6, 2021 to A.D., a U.S. Army Recruiter in Cedar Hills, Texas.

1. The identity of the person(s) who created or used the account, including records that help reveal the whereabouts of such person(s);
2. Evidence indicating how and when the account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the offenses under investigation and to the account owner(s);
3. Evidence indicating the owner of the account's state of mind as it relates to the crimes under investigation;
4. The identity of any person(s) who communicated with the account about the crimes under investigation, including the identity and whereabouts of co-conspirators, accomplices, and aiders and abettors in the commission of the criminal activity under investigation;

5. Records concerning the identity and role of person(s) who collaborated, conspired, or assisted (knowingly or unknowingly) with the commission of the crimes under investigation, including records that help reveal their whereabouts;
6. Records related to communications with any individual from the U.S. Army, or any attempt to contact a recruiter with the U.S. Army in Cedar Hills, Texas, such as A.D.;
7. Records related to any racial animus or extremist ideology of the user of the Target Account;
8. Records related to the purchase of any firearms, explosives, or other dangerous weapons to carry out any threats;
9. Records related to the identity of any victim of a threatening communication sent or received using the Target Account.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.